(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 November 2003 (20.11.2003)

PCT

(10) International Publication Number
WO 03/096263 A1

(51) International Patent Classification[7]: G06K 9/00

(21) International Application Number: PCT/SE03/00729

(22) International Filing Date: 7 May 2003 (07.05.2003)

(25) Filing Language: Swedish

(26) Publication Language: English

(30) Priority Data:
0201366-2 7 May 2002 (07.05.2002) SE

(71) Applicant *(for all designated States except US)*: **PRECISE BIOMETRICS AB** [SE/SE]; Scheelevägen 19C, S-223 70 Lund (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **NORDIN, Björn** [SE/SE]; Kollegievägen 2, S-223 74 Lund (SE).

(74) Agent: **AWAPATENT AB**; Box 5117, S-200 71 Malmö (SE).

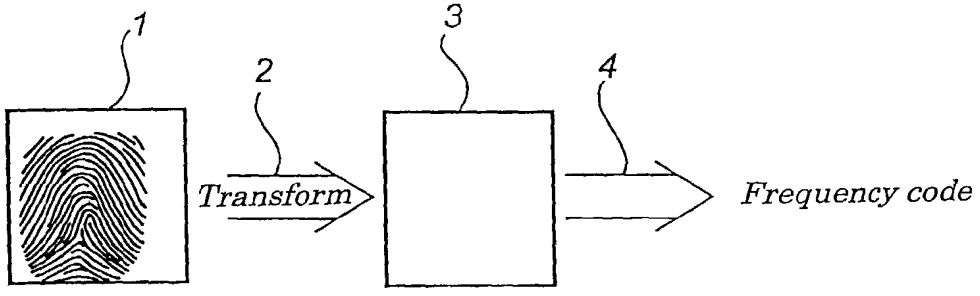
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND DEVICES FOR IDENTITY CHECK



(57) Abstract: In a method for use in checking a person's identity, at least part of an image of a fingerprint from the person is transformed so that a representation of a frequency content in said part of the image is obtained. Based on the obtained representation of the frequency content, a frequency code is determined, which contains a predetermined number of frequency code values. A device for carrying out the method is also described.

WO 03/096263 A1

METHOD AND DEVICES FOR IDENTITY CHECK

Field of the Invention

The present invention relates to a method and a device for use in checking a person's identity.

Background Art

It is known to use fingerprints for checking a person's identity. In such a check, current data from a current fingerprint from the person whose identity is to be checked is compared with previously recorded reference fingerprint data (below sometimes only called reference data) for one or more persons.

If the check concerns a verification of the person's identity, the current data from the current fingerprint is compared only with reference data for the person who the person whose identity is to be checked pretends to be.

If the check concerns an identification of the person's identity, the current data is compared with reference data for at least two, but usually several, different persons to determine whether the current fingerprint originates from any of these persons.

Reference fingerprint data for a plurality of persons can be stored in a local database for an individual fingerprint checking system or in a central database for a plurality of checking systems. Alternatively, reference data for a person can be stored in a personal unit, such as a personal memory card or smart card, which the person uses when he or she wants to authenticate himself/herself, i.e. prove his/her identity by verification or identification.

In some types of storing units there may be a limited storage capacity. In such cases it is desirable to have a small amount of reference data.

The comparison between reference data and current data can be made either in the same physical unit as the one in which the reference data is stored, in the same physical unit as records and processes the current fingerprint or in some other unit.

If the comparison is made in a unit with a limited processor capacity, it is desirable that the comparison between current data and reference data can be made in a simple way. If either current data or reference data has to be transferred from one unit to another in connection with the comparison, it is desirable for the amount of data to be small so that the transfer time will be short.

In many applications, the user wants to be able to authenticate himself and get access to a protected object without delay. Then it is desirable that the current data can be generated quickly, that the transfer time, if any, is short and that the comparison can be made quickly.

The reference data can correspond to a complete fingerprint as recorded. However, only part of the information in the fingerprint is usually saved as reference data.

For instance, it is known to save as reference data information about specific features, also referred to as minutiae points, in the fingerprint. These specific features are usually of two predetermined types, viz. fingerprint ridge endings and fingerprint ridge bifurcations. For instance, coordinates for where these features are placed can be saved as reference data. When checking a person's identity, the relative location of features in a current fingerprint is determined and then compared with the relative location of the features in the reference data.

From, for instance, WO 01/84494 it is also known to save as reference data partial areas of an image of a reference fingerprint. When checking a person's identity, corresponding partial areas are found in a current fingerprint and then compared with the partial areas in

the reference data. To allow the final identity check to be carried out on a smart card with a limited processor and memory capacity, a partial area is stored as a so-called public partial area in a public part of the reference data on the smart card. In the identity check, this public partial area is read to a computer unit, in which it is compared with a current fingerprint to determine in which position in relation to this the public partial area fits best. In this way, the reference data is aligned with the current fingerprint. In the public part of the reference data, also coordinates for how other partial areas, so-called private partial areas, are placed in relation to the public partial area are stored. When the current fingerprint has been aligned with the reference data, these coordinates can be used to determine which partial areas in the current image are to be selected and sent to the smart card for comparison with the private partial areas.

It is further known to form a finger code by first finding an objective reference point in a fingerprint, then dividing the fingerprint into sectors in relation to the reference point, then Gabor filtering the image with a number of Gabor filters and finally calculating the finger code as the variance in each sector of the Gabor-filtered image. The obtained finger code is advantageous as reference data since it will be quick and easy to compare a reference finger code with a current finger code. However, it takes relatively long to find the finger code. Another problem is that it is based on the fact that an objective reference point can be established in the fingerprint merely by searching in the same. It is known, however, that for certain fingerprints it is difficult, not to say impossible, to establish such an objective reference point.

Summary of the Invention

An object of the invention is to provide a method and a device for use in checking a person's identity,

which method and which device make it possible to wholly or partly satisfy one or more of the above desiderata as regards storage space, transfer time, comparison time and time for generating data.

More specifically, according to the invention, a method is provided for use in checking a person's identity, comprising the steps of transforming at least part of an image of a fingerprint from the person so that a representation of a frequency content in said part of the image is obtained, and based on the obtained representation of the frequency content, determining a frequency code which contains a predetermined number of frequency code values.

There are techniques, for instance Fourier transforming, which make it possible to quickly transform an image so that a representation of the frequency content in the image is obtained. Based on this representation, a frequency code can be determined relatively quickly and easily. It is also possible to generate reference data and current data in a time which is acceptably short for many applications.

Depending on how many frequency code values the frequency code contains and how the frequency code values are defined, it is possible to produce reference data and current data requiring a small storage space and short transfer time, but still giving a probability of error which is acceptably low for many applications regarding errors of type 1 (that a current fingerprint from the same person and finger as those from which the reference data is fetched is not accepted) and of type 2 (that a current fingerprint from another person or another finger than the one from which the reference data is fetched is accepted).

As mentioned above, the method according to the invention is intended for use when checking a person's identity. This may comprise, for instance, that the method is used for producing reference fingerprint data

for a person, for producing current fingerprint data or for checking a person's identity.

The image can be a grey-scale image, a binary image or a colour image. It shows a fingerprint by representing ridges and valleys in the fingerprint with different intensities. The image may comprise a complete fingerprint or a partial fingerprint depending on the size of the sensor that has been used to record the image.

By the image or part of this being transformed is here meant that a mathematically defined transform is allowed to operate on the image and convert the information in the image into a representation of the frequency content, i.e. with which frequencies it is possible to describe the intensity variations in the image in different directions and the mutual relationship thereof.

In some cases, it may be desirable to transform only part of the fingerprint image. It may be desirable, for instance, to exclude the background or parts where the fingerprint is of poor quality, it may be desirable to use only an area round a certain point, or it may for some other reason be desirable to select only a part to be transformed.

The frequency code contains a predetermined number of frequency code values. The number of values in the code can be determined from the desired size of the reference data and the desired probability of error of types 1 and 2. A greater number of values requires a greater storage capacity for the reference data, but normally gives lower probability of error.

The transform can be, for instance, one, or a combination, of the following transforms: Fourier transforms, Cosinus transforms, Bessel transforms or Hadamard transforms. An advantage of these transforms is that they are to some extent insensitive to lateral displacements of a finger on a sensor as long as the same part of the finger is located on the sensor.

The frequency code values are determined based on the obtained representation of the frequency content. More specifically, they can be determined based on a predetermined number of frequency values that are selected from the representation of the frequency content, in which case each frequency value may be a measure of the existence of a corresponding frequency in a certain direction in the image that is transformed. One or more frequency values can be used to produce a frequency code value. A plurality of frequency values can, for instance, be averaged or weighted together to determine a frequency code value.

The method according to the invention can be accomplished by means of a computer program. The computer program can be stored on a storage medium, for instance in a memory of electronic, optical, magnetic or some other known type. The storage medium can also be a propagating signal.

According to another aspect of the invention, a device is provided for use in checking a person's identity, comprising a signal processor, which is adapted to transform at least part of an image of a fingerprint from the person so that a representation of a frequency content in said part of the image is obtained, and based on the obtained representation of the frequency content, determining a frequency code which contains a predetermined number of frequency code values.

The signal processor can be accomplished by means of a suitably programmed general or specially adapted computer. It can alternatively be accomplished with specially adapted hardware, such as an ASIC (Application Specific Integrated Circuit) or with an FPGA (Field Programmable Gate Array) or with analog circuits or digital circuits or with a suitable combination thereof.

Brief Description of the Drawings

The present invention will now be described in more detail by way of example and with reference to the accompanying drawings, in which

Fig. 1 shows most schematically the basic principle of the present invention;

Fig. 2 shows an example of a system in which an identity check by means of frequency codes can be performed;

Fig. 3 shows an image of a fingerprint;

Fig. 4 shows a representation of the frequency content in the fingerprint in Fig. 3;

Fig. 5 is a flow chart and shows an example of a method for producing reference fingerprint data; and

Fig. 6 is a flow chart and shows an example of a method for identity checking.

Detailed Description of Embodiments

The present invention is based on the idea of generating a frequency code that can be used when checking a person's identity. This is schematically illustrated in Fig. 1.

First, an image 1 of a fingerprint from a person is recorded. This image represents the information in the fingerprint in the form of intensity variations. The image 1 is transformed 2 so that a representation 3 of the frequency content in the image 1 is obtained instead.

From this frequency representation, a number of frequency values is selected and processed 4 so that they can be represented in a compact way in the form of frequency code values. The frequency code values jointly form a frequency code C_R. This frequency code can be stored as reference fingerprint data to be used in a subsequent identity check.

In the identity check, a current frequency code C_A is generated from a current fingerprint and compared with the previously stored reference frequency code C_R. If the compared frequency codes are sufficiently equal,

the fingerprints from which they are generated will be considered to originate from one and the same finger, and thus the person's identity is ensured.

In the following, an example of a system will be described, in which an identity check by means of frequency codes can be performed. The system comprises, as shown in Fig. 2, a fingerprint sensor 10 for recording fingerprints, a first unit 11, which in the following is called computer unit, for processing fingerprint data, and a second unit 12, which comprises a memory for storing reference fingerprint data and a processor for processing fingerprint data and which in this case consists of a smart card.

The sensor 10 can, but need not, be used both for recording of reference fingerprints and for recording of current fingerprints. It can be optical, capacitive, thermal or be of some other convenient type. It can be an area sensor or a line sensor.

The computer unit 11 can be a common general computer, such as a PC. Alternatively, it can be, for instance, a computer unit 11 which is specially adapted for this application or specially adapted hardware. In this example, it comprises a smart card reader 13, which may be any commercially available smart card reader or a specially designed/adapted smart card reader. The smart card reader 13 may be physically integrated into the computer unit 11 or may be arranged in a casing of its own which in terms of signals is connected or connectible to the rest of the computer unit. There may be one or more processors in the computer unit 11, and the processing of fingerprint data that takes place in the computer unit can be distributed in different ways among different processors.

The smart card 12 can be any type of smart card on which a comparison of fingerprint data is to be carried out. The smart card 12 has a signal processing unit which comprises a processor 16, a memory 17 for storing of

reference fingerprint data which is extracted from a reference fingerprint from the smart card holder, and a working memory 18, as well as communication circuits 19 which enable communication between the smart card reader 13 and the smart card 12. The communication circuits 19 can, but need not, require contact between the smart card 12 and the reader 13.

In the following, an example of how the invention can be realised in the system shown in Fig. 2 will be described.

To allow the smart card 12 to be used to verify the smart card holder's identity, reference fingerprint data must be stored in the memory 17 of the smart card. This is preferably carried out under such conditions that it is possible to ensure that it is really the smart card holder's reference fingerprint data that is stored. An example of how the recording of reference fingerprint data is made is shown in the flow chart in Fig. 5.

In a first step 50, an image of the smart card holder's fingerprint is recorded by means of a sensor 10. An example of how a real fingerprint image that has been recorded by means of a capacitive fingerprint sensor is shown in Fig. 3. In the image, the dark lines correspond to ridges in the fingerprint and the light lines to valleys in the fingerprint. The darker portions that are found in the upper and lower edge of the image are caused by remaining layers of fat on the sensor.

The image is read from the sensor 10 into the computer unit 11 where it is Fourier transformed, step 51. The Fourier transformation can be made by means of specially developed software or hardware or by means of commercially available software or hardware. It is normally made by means of calculations based on a mathematical method, but can also be made without calculations using an optical lens and a sensor. Optionally, only part of the image can be selected and transformed.

By the Fourier transformation, frequency values F(u,v) are obtained, which consist of complex numbers with a real part and an imaginary part as follows

$$F(u,v) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\exp\left[-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right]$$

where u=0,1,2,...,M-1
v=0,1,2,...,N-1

and where u and v are Cartesian coordinates in the Fourier transformed image and x and y are Cartesian coordinates in the fingerprint image (Fig. 3).

The frequency values F(u,v) constitute a representation of the frequency content in the fingerprint image. The frequency content can be illustrated in an image.

Fig. 4 shows a Fourier transform of the image in Fig. 3. More specifically, the absolute values of the frequency values F(u,v) are shown. Fig. 4 shows a grey-scale image of what frequencies exist in different directions in the fingerprint in Fig. 3, the frequency increasing as a function of the radius r in Fig. 4, the angle θ from the horizontal axis A in Fig. 4 indicating the direction in Fig. 3 and higher existence of a certain frequency being illustrated in lighter grey-scale in Fig. 4. The representation in Fig. 4 is symmetrical since the frequency content will be the same in directions that differ by 180 degrees.

For each frequency in Fig. 4 there is thus a frequency value which gives a measure of the existence of the frequency in the current direction v. These frequency values are used to generate the frequency code. More specifically, a predetermined number of frequency values is selected, step 52.

Fig. 4 shows all frequencies within a certain frequency range, i.e. also frequencies that are not significant to a fingerprint since they do not at all reflect the closeness of fingerprint lines in different direc-

tions in a fingerprint. Therefore the frequency values are selected for frequencies within a limited range in Fig. 4, which range is relevant for fingerprints. In Fig. 4, frequencies are selected in the upper semi-plane in the annular area between the radii R_1 and R_2.

The relevant range is individual-dependent since different people have different spacings between the fingerprint lines. The frequency values can then be selected either for frequencies within a large predetermined range taking the distribution among different individuals into consideration, or for frequencies within a smaller individual-adapted range. The individual-adapted frequency range is determined as a range in which the individual in question has a high existence of relevant frequencies, i.e. frequencies corresponding to structures in the fingerprint.

For instance, the frequency range can in the former case be selected so as to correspond to 800 to 5000 lines/m.

For determining the frequency code values, either the real parts, the imaginary parts, the absolute values or a combination thereof can be used, for instance phase displacement.

In this example, it is assumed that the absolute values (also called magnitudes) of the selected frequency values are calculated, step 53.

The frequency code C is generated by the sequence of the thus generated frequency code values. Expressed in a different way:

$$C(r,v) = |F(r,\theta)| \qquad \text{where } R_1<r<R_2 \text{ and } 0<v<\pi$$

where $F(r,\theta)$ is the frequency value in the point (r,θ) and $C(r,\theta)$ is the frequency code value for the same point.

With this terminology, it is thus the frequency code values $C(r,\theta)$ that are shown in Fig. 4. Thus it is pos-

sible, as an alternative, first to calculate the frequency code values for all points and then select frequency code values for predetermined frequencies as the frequency code values to form to the frequency code.

For the frequency code to be represented in a memory-saving manner, the frequency code values $C(r,\theta)$ are then quantisised, step 54, for instance to one of the values 0, 1, 2 or 3.

If 800 frequency values are selected, for instance 20 different frequencies for each of the 40 different angles v, a frequency code C_R with 200 byte data will be obtained if the frequency code values are quantisised as described above.

The values are stored in a table with 5 bytes in each row. This means that each row contains the quantisised frequency code values for an angular value. A change of the frequency code corresponding to a turning of the fingerprint in either direction at an angle of 4.5 degrees can thus easily be achieved. The only thing that need be made is to circular-shift the rows in the table one step in the corresponding direction.

Finally, the frequency code C_R is stored, step 55, as reference fingerprint data on the smart card 12. As will be described in more detail below, the frequency code can be stored as public reference fingerprint data that is allowed to be read from the smart card for use in the computer unit in an identity check, or as private reference fingerprint data that is not allowed to be read from the smart card but is compared with current fingerprint data on the smart card.

Once reference fingerprint data has been stored on the smart card 12, the smart card holder can use the smart card to authenticate himself. An example of how this may be done will be described in the following.

The smart card holder inserts his smart card 12 in the smart card reader 13 and places the same finger

on the sensor 1 as was used for recording of reference fingerprint data on the sensor 10.

The sensor 10 records a current image of the smart card holder's fingerprint, step 60 in Fig. 6. The image is read into the computer unit 11 where it is processed in exactly the same way as in the recording of the reference fingerprint data. More specifically, the image is Fourier transformed, step 61, frequency values are selected in the image, step 62, the absolute values of the selected frequency values are calculated, step 63, and the calculated absolute values are quantisised, step 64, to form the current frequency code C_A.

As an alternative, the frequency values can be selected within a predetermined, individual-independent range. This alternative may be used even if the reference frequency code is based on an individual-dependent range since in that case a greater current frequency code can be sent to the smart card and a suitable subset of the current frequency code can be selected on the smart card based on data stored there regarding on what frequency range the reference frequency code is based.

As another alternative, the frequency values can be selected individual dependent. The frequency range may then be selected depending on where in the representation of the frequency content in the current fingerprint the individual has high existences of frequencies. Alternatively, the frequency range may be selected based on data about this that is sent from the smart card.

The current frequency code C_A is sent to the smart card 12 where it is compared, step 65, with the previously stored reference frequency code C_R. The comparison is made by determining the absolute difference between frequency code values corresponding to each other. The total difference is then compared, step 66, with a threshold value to determine whether a similarity condition is satisfied and whether the reference frequency code C_R and

the current frequency code C_A can thus be considered to originate from one and the same finger.

In the recording of the current fingerprint it may happen that the person in question places his finger at a different angle on the sensor compared with the recording of the reference fingerprint. This will affect the frequency code by the representation of the frequency content being rotated. The frequency code values will thus be in a different order in the frequency code. In the identity check, this can be taken into consideration by repeating the comparison between the current frequency code and the reference frequency code with a mutual permutation of the frequency code values, step 67. The mutual permutation can be effected in various ways; the processor on the smart card can permute the values either in the reference frequency code or in the current frequency code so that the permutation corresponds to a certain degree of rotation or, alternatively, the reference frequency code can be stored on the smart card in different versions with the frequency code values permuted. As another alternative, the computer unit 11 can generate different versions of the current frequency code and send them to the smart card for comparison.

In the case when several comparisons are made, the criterion for identifying a person will be that one of the permutations satisfies the similarity criterion.

However, the permutation need not always be effected. Some fingerprint sensors have different control means which command the user to always place his finger in the same position on the sensor. When using such a fingerprint sensor, the frequency code thus need not be permuted.

It may also happen that the user when recording the current fingerprint places his finger in the same rotational position on the sensor but in a translated position. Since the frequency code is based on the frequency content, which is a global property of the fingerprint,

the translation will have a smaller effect on the frequency code compared with the case of using minutiae points and partial areas representing local properties in the fingerprint.

An embodiment has been described above where the current frequency code is generated in the computer unit and then compared with a reference frequency code on the smart card. In this case, the reference frequency code never leaves the smart card and therefore constitutes private reference fingerprint data.

However, it is also conceivable to use the reference frequency code as public reference fingerprint data which is allowed to be read from the smart card for use in the computer unit for alignment of the current fingerprint image with the private reference fingerprint data so that the final comparison between current fingerprint data and reference fingerprint data will be easier and quicker to perform.

More specifically, in this case the reference fingerprint code is thus stored as public reference data. If the reference fingerprint code is based on the absolute values of the frequency values, alignment can only be made in the rotational direction. On the other hand, if the reference fingerprint code contains both quantisised real parts and quantisised imaginary parts of the frequency values, alignment may however also be made in the translational direction.

Moreover, other fingerprint data is stored as private reference data on the smart card. This other fingerprint data may consist of a fingerprint code which is based on other points in the representation of the frequency content, partial areas of the reference fingerprint image, minutiae points from the reference fingerprint image or some other fingerprint data which is determined from the reference fingerprint image.

In the identity check, a current image of the fingerprint from the person whose identity is to be

checked is recorded in the same way as before. The current image is Fourier transformed as described above. The computer unit further reads the public reference fingerprint data from the smart card, i.e. in this case the reference frequency code $C_R(r,\theta)$. Each complex value of the Fourier transform is then multiplied by the corresponding complex value in the reference frequency code $C_R(r,\theta)$ as follows

$$G(r,\theta) = F(r,\theta) * C_R(r,\theta) .$$

According to the correlation theorem, this multiplication corresponds to a correlation of two images in the spatial plane.

After that $G(r,\theta)$ is inverse Fourier transformed back to the spatial plane to g. The coordinates for the maximum value of g then immediately corresponds to the relative translation between the reference fingerprint image and the current fingerprint image. If these are not displaced in relation to each other, the maximum value of g would thus be in the centre of g.

The rotation between the current image and the reference image can further be determined by permutation of the reference frequency code and a current frequency code which is generated from the Fourier transform in the same way as described above. Once the rotation and the translation have been determined, the current fingerprint image and the reference fingerprint image have thus been aligned with each other. Starting from the alignment, data from the current image can be more easily compared with reference data on the smart card.

If the private reference data consists of partial areas, the current partial areas can be determined after the alignment has been made by means of the frequency code. If the private reference data consists of minutiae points, coordinates for these can be determined in the

coordinate system of the reference data after alignment by means of the frequency code.

As a further alternative, comparison by means of the frequency code can be carried out supplementing a comparison between some other type of fingerprint data. Since the frequency code reflects a global property of the fingerprint, it may be convenient to make a supplementary comparison of a local property, for instance minutiae points or partial areas. This should increase safety in the authentication. The criterion for the current person's identity to be considered authenticated can be that an authentication threshold value should be achieved separately for both comparisons of the fingerprint data or be achieved for only one comparison. Alternatively, it is possible to use some kind of criterion which is based on a weighting of the authentication threshold values for both comparisons.

An embodiment has been described above where the frequency code is generated in a computer unit and where the comparison takes place on a smart card. It is possible, however, to realise the invention by means of some other pair of a first and a second unit. The first unit may be, for instance, a PC of an Internet customer and the second unit a computer of a service provider which stores the reference fingerprint data under safe conditions. As a further example, the first unit may consist of a mobile phone and the second unit of a SIM card or the like in the mobile phone. It is also conceivable that the method can be realised wholly or partly in some other type of portable unit, such as a PDA, a pen provided with a processor, or an access protected hard disk.

It is alternatively conceivable to carry out the method described above by determining a current frequency code and comparing the current frequency code with a reference code in one and the same unit.

A further conceivable application is to use the frequency code in identification. The current frequency code

is then compared with reference frequency codes for a number of people. The purpose is then to select in a first step a small number of the people as candidates for additional comparison. The additional comparison can then be made by means of some other type of reference fingerprint data, for example minutiae points or partial areas.

CLAIMS

1. A method for use in checking a person's identity, comprising the steps of

transforming at least part of an image of a fingerprint from the person so that a representation of a frequency content in said part of the image is obtained, and

based on the obtained representation of the frequency content, determining a frequency code which contains a predetermined number of frequency code values.

2. A method as claimed in claim 1, wherein the step of transforming is performed by means of at least one transform from the group of Fourier transforms, Cosinus transforms, Bessel transforms and Hadamard transforms.

3. A method as claimed in claim 1 or 2, comprising selecting, from the representation of the frequency content, a predetermined number of frequency values, and determining said frequency code values based on the frequency values.

4. A method as claimed in claim 3, wherein the frequency values selected are frequency values of predetermined frequencies.

5. A method as claimed in claim 3, comprising selecting, in the representation of the frequency content, an individual frequency range for the person, said predetermined number of frequency values being selected for frequencies in the selected frequency range.

6. A method as claimed in any one of claims 3-5, comprising calculating the absolute value of at least one of the selected frequency values and using the absolute value for determining one of said frequency code values.

7. A method as claimed in any one of claims 3-6, comprising using, for at least one of the selected frequency values, the real part of the selected frequency value for determining one of said frequency code values.

8. A method as claimed in any one of claims 3-7, comprising using, for at least one of the selected frequency values, the imaginary part of the selected frequency value for determining one of said frequency code values.

9. A method as claimed in any one of claims 3-8, wherein the determination of said frequency code values comprises quantisising the selected frequency values.

10. A method as claimed in any one of the preceding claims, wherein the frequency content is represented in polar coordinates.

11. A method as claimed in any one of the preceding claims, comprising storing the frequency code as reference fingerprint data for the person.

12. A method as claimed in claim 11, wherein the reference fingerprint data is stored on a portable data carrier, preferably a smart card.

13. A method as claimed in claim 11 or 12, wherein the reference fingerprint data is stored in a unit as public reference fingerprint data that is allowed to be read from the unit.

14. A method as claimed in claim 11 or 12, wherein the reference fingerprint data is stored in a unit as private reference fingerprint data that is not allowed to be read from the unit.

15. A method as claimed in any one of claims 1-10, wherein the frequency code is compared with at least one reference frequency code which contains a predetermined number of frequency code values.

16. A method as claimed in claim 14, comprising repeating the comparison between the frequency code and the reference frequency code with a mutual permutation of the frequency code values.

17. A method as claimed in claim 14, further comprising the step of permuting the frequency code values in either the frequency code or the reference frequency code and repeating the comparison.

18. A method as claimed in any one of claims 14-16, wherein the frequency code is determined in a first unit and the comparison with the reference frequency code takes place in a second unit.

19. A method as claimed in any one of claims 14-16, wherein the frequency code is determined in a first unit, the reference frequency code is received from a second unit, the frequency code is compared with the reference frequency code and other data from the image is sent to the second unit based on the result of the comparison between the frequency code and the reference frequency code.

20. A method as claimed in any one of claims 14-19, wherein the frequency code is compared with a plurality of reference frequency codes for different people, and a small number of said different people is selected for further checking.

21. A computer program product, on which a computer program is stored with instructions for carrying out a method as claimed in any one of claims 1-20.

22. A device for use in checking a person's identity, comprising a signal processor which is adapted to

transform at least part of an image of a fingerprint from the person so that a representation of a frequency content in said part of the image is obtained, and

based on the obtained representation of the frequency content, determine a frequency code which contains a predetermined number of frequency code values.

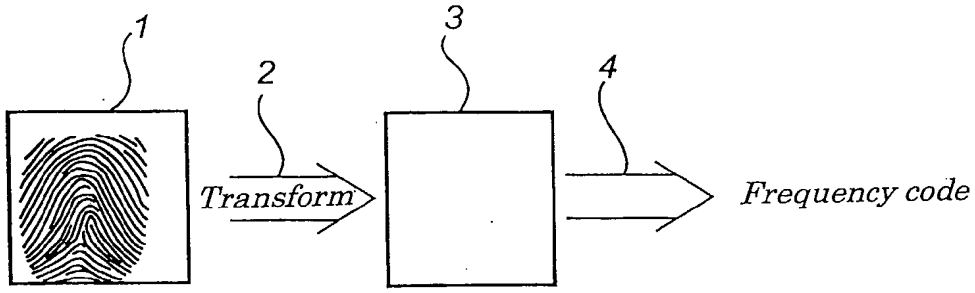


Fig. 1

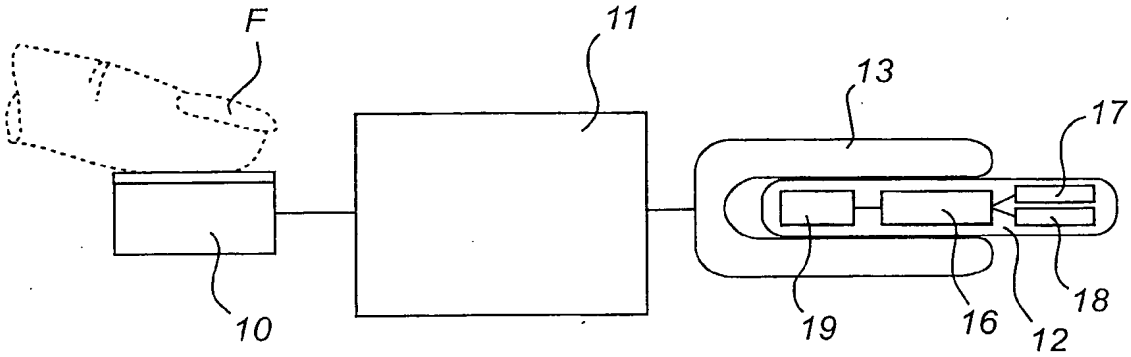


Fig. 2

Fig. 3

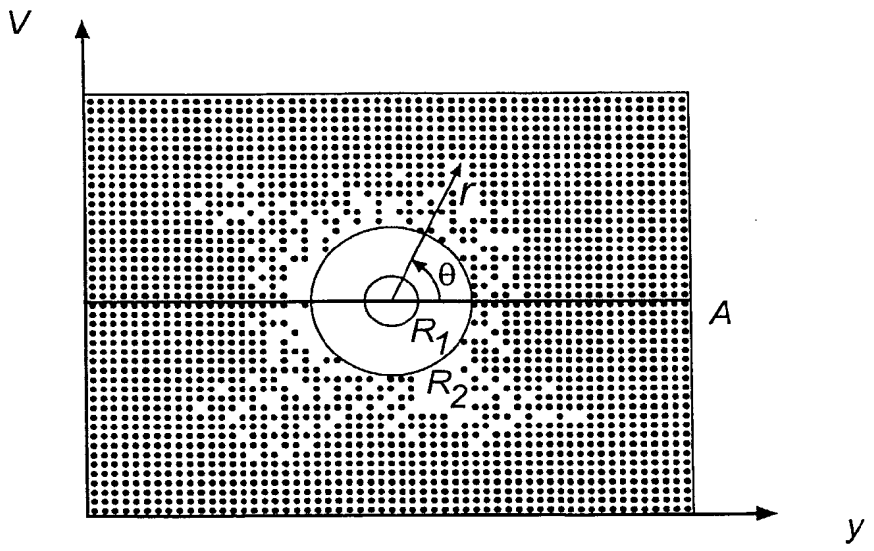


Fig. 4

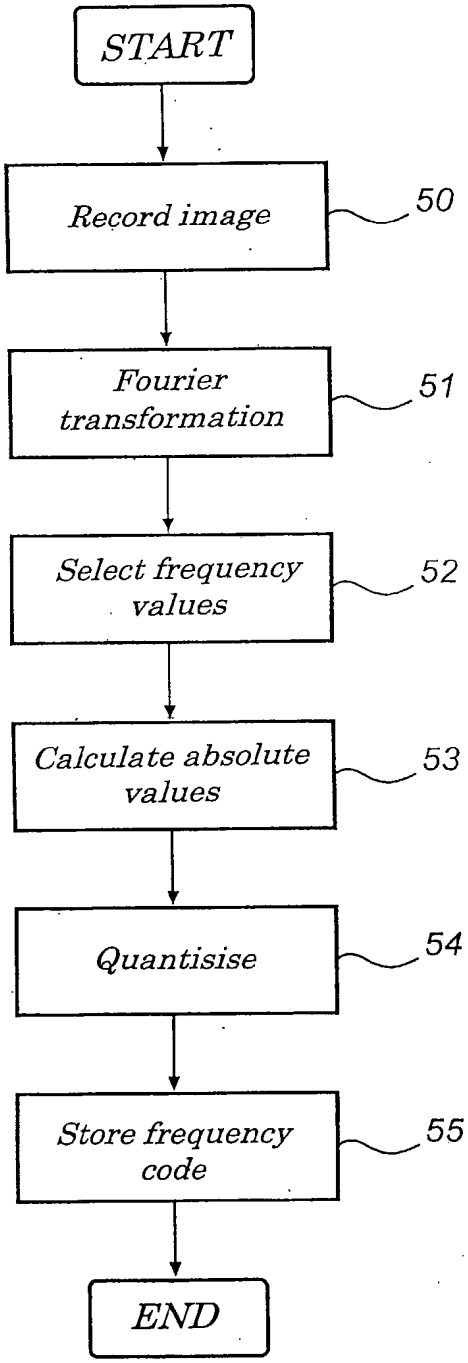

START
Record image
50
Fourier transformation
51
Select frequency values
52
Calculate absolute values
53
Quantisise
54
Store frequency code
55
END

Fig. 5

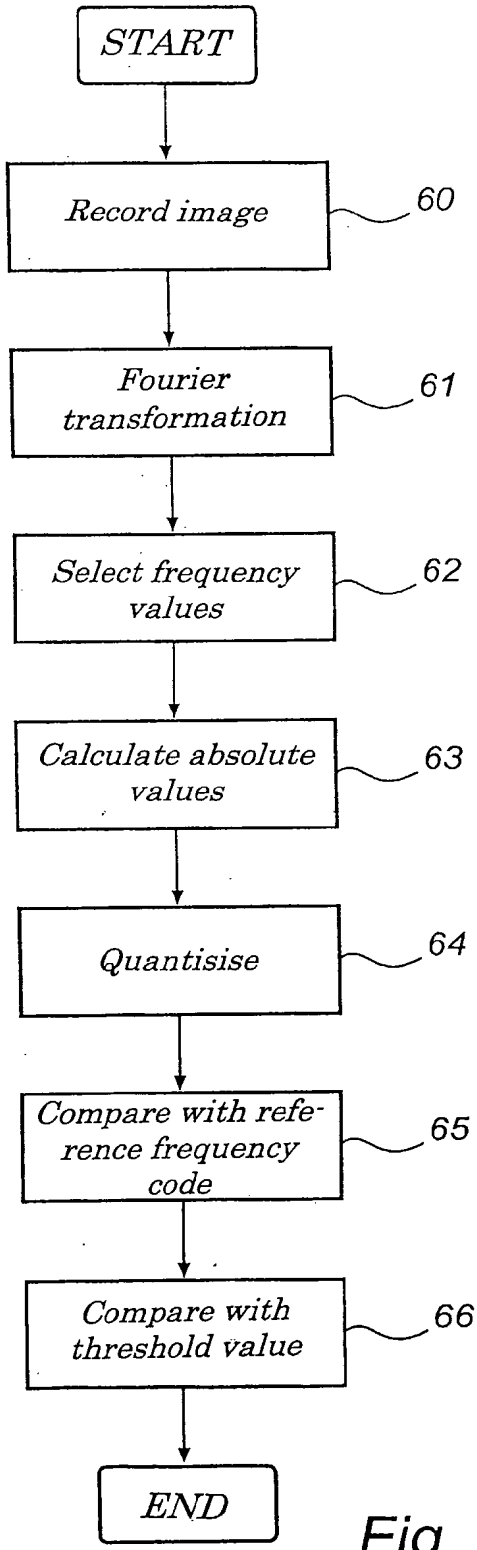

START
Record image
60
Fourier transformation
61
Select frequency values
62
Calculate absolute values
63
Quantisise
64
Compare with reference frequency code
65
Compare with threshold value
66
END

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 03/00729

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G09K 9/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06K, A61B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ, INSPEC, TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0778541 A2 (HAMAMATSU PHOTONICS K.K.), 20 November 1996 (20.11.96), page 4, line 1 - line 57, abstract --	1-22
A	US 5426708 A (HAMADA, T. ET AL), 20 May 1995 (20.05.95), column 1, line 55 - column 2, line 29, figures 5,6, abstract --	1-22
A	US 5761330 A (STOIANOV, A. ET AL), 2 June 1998 (02.06.98), column 1, line 58 - column 2, line 7; column 3, line 33 - line 45, abstract --	1-22

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 July 2003	18 -07- 2003
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Alexander Lakic/mj Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 03/00729

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9904358 A1 (KABA SCHLIESSSYSTEME AG), 28 January 1999 (28.01.99), abstract ---	1-22
A	US 4805223 A (DENYER, P.B.), 14 February 1989 (14.02.89), abstract ---	1-22
A	EP 0329166 A2 (NIPPONDENSO CO, LTD), 17 February 1989 (17.02.89), abstract --- --------	1-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

29/06/03

International application No.
PCT/SE 03/00729

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0778541 A2	20/11/96	DE 69608218 D,T	07/09/00
		JP 9147115 A	06/06/97
		US 5910999 A	08/06/99
US 5426708 A	20/05/95	DE 4324296 A,C	10/02/94
		JP 3057590 B	26/06/00
		JP 6060167 A	04/03/94
US 5761330 A	02/06/98	AU 5889196 A	30/12/96
		WO 9641297 A	19/12/96
WO 9904358 A1	28/01/99	AT 237163 T	15/04/03
		AU 761123 B	29/05/03
		AU 8203998 A	10/02/99
		BR 9811511 A	12/09/00
		CN 1271446 T	25/10/00
		DE 59807883 D	00/00/00
		EP 0996924 A,B	03/05/00
		JP 2001510920 T	07/08/01
US 4805223 A	14/02/89	EP 0218668 A	22/04/87
		GB 2174831 A,B	12/11/86
		GB 8609673 D	00/00/00
		JP 62502575 T	01/10/87
		WO 8606527 A	06/11/86
EP 0329166 A2	17/02/89	DE 68918724 D,T	24/05/95
		JP 1209585 A	23/08/89
		JP 2067303 C	10/07/96
		JP 7104942 B	13/11/95
		US 5040223 A	13/08/91
		JP 1283674 A	15/11/89